UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,424	08/30/2000	Mariusz H. Jakubowski	MS1-528US	2561

22801	7590	05/05/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
TRAN, TONGOC

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _30 August 2000_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-36_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-36_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _3_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____ .

DETAILED ACTION

1.   This office action is in response to applicants' application serial no.

09/665,424 filed on 8/30/2000.

Information Disclosure Statement

2.   The information disclosure statement (IDS) submitted on 6/13/2003 has

been considered by the examiner.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 and 8-13 and 15-30 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Merkle (U.S. Patent No. 5,003,597) in view of Chow

(U.S. Patent No. 6,594,761).

In respect to claim 1, Merkle discloses one or more computer readable

media having stored thereon a plurality of instructions that, when executed by

one or more processors, causes the one or more processors to perform acts

including:

selecting a portion of clear text blocks (see Merkle, col. 2, lines 52-63);

selecting another portion of the digital good, wherein the other portion is to be encrypted; and using the portion as a substitution box (S-box) when encrypting the other portion (see Merkle, Fig. 1, col. 2, line 51-col. 3, line 21).

Merkle does not explicitly discloses said clear text is digital good. However, Chow discloses using DES technique to obfuscate digital good for tamper resistant protection (see Chow, col. 10, lines 6-15 and col. 20, lines 29-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Merkle's encryption technique with Chow's teaching of using DES to obfuscate software program to ensure program of computer software needs to be protected is tamper resistant (Chow, col. 10, lines 10-14).

In respect to claim 2, Merkle and Chow disclose one or more computer readable-media as recited in claim 1, wherein the entire digital good is to be encrypted (see Chow, col. 10, lines 1-15).

In respect to claim 3, Merkle and Chow disclose one or more computer readable media. as recited in claim 1, wherein the using comprises determining, for each group of bits of the other portion, a new group of bits based on the portion (see Merkle, col. 2, line 51-col. 3, line 35).

In respect to claim 4, Merkle and Chow disclose one or more computer readable media as recited in claim 1, wherein the using comprises using bits of the portion to determine a substitution sub portion for each sub-portion in the other portion (see Merkle, col. 2, line 51-col. 3, line 35).

In respect to claim 5, Merkle and Chow disclose one or more computer readable media as recited in claim 4, wherein the sub-portion comprises a byte (see Merkle, col. 3, lines 22-35).

In respect to claim 6, Merkle and Chow disclose one or more computer readable media as recited in claim 1, wherein the digital good comprises a software program (see Chow, col. 10, lines 6-15).

In respect to claims 8, 10, 17-18, the claim limitations method claims that are substantially similar to claim 1. Therefore claims 8, 10, 17-18 are rejected based on the similar rationale.

In respect to claims 9, 11-13 and 19-22, the claim limitations are method claims that are substantially similar computer readable medium claims 2-3, 4 and 6. Therefore claims 9, 11-13 and 19-22 are rejected based on the similar rationale.

In respect to claims 15 and 23, A method as recited in claims 8 and 17, wherein the encryption process uses a Data Encryption Standard (DES) cipher.

In respect to claim 16, the claim limitation is a computer readable medium that is substantially similar to claim 1. Therefore, claim 16 is rejected based on the similar rationale.

In respect to claim 24, the claim limitation is a computer readable medium claim that is substantially similar to method claim 17. Therefore, claim 24 is rejected based on the similar rationale.

4.   Claims 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Merkle (U.S. Patent No. 5,003,597) in view of Sirbu (U.S. Patent No.

5,809,144).

In respect to claim 31, Merkle discloses comprising:

Selecting portion of clear text as a substitution box (S-box) in encrypting at least

a portion of a second portion of clear text to produce encrypted text (see col. 2,

line 52-col. 3, line 35). Merkle does not disclose but Sirbu discloses a server

production encrypts digital good; and a client to store and execute the protected

digital good, the client being configure to evaluate the protected digital to

determine whether the protected digital good has been tampered with (see col. 9,

lines 30-37). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to implement the teaching of Merkle's

encryption technique with the teaching of Sirbu's client's verifying received digital

good to ensure that content of the digital good is received completely and

correctly (Sirbu, col. 10, lines 9-11).

In respect to claim 32, Merkle and Sirbu discloses a client-server system

as recited in claim 31, wherein the first digital good and the second digital good

are the same digital good (see Merkle, col. 2, lines 50-63).

In respect to claim 33, Merkle and Sirbu disclose one or more computer

readable media having stored thereon a plurality of instructions that, when

executed by one or more processors, causes the one or more processors to

perform acts including:

decrypting at least a portion of a digital good by using another portion of

the digital good as a substitution box (S-box) (see Merkle, col. 2, line 51-col. 3,

line 21).

In respect to claim 34, Merkle and Sirbu disclose one or more computer

readable media as recited in claim 33, wherein the decrypting is based at: least

in part on a Data Encryption Standard (DES) cipher (see col. 3, lines 6-21).

In respect to claim 35, Merkle and Sirbu disclose one or more computer

readable media as recited in claim 33, wherein the decrypting comprises using

bits of the other portion to determine a substitution value for each value in the

portion (see col. 2, line 51-col. 3, line 21).

In respect to claim 36, Merkle and Sirbu disclose one or more computer

readable media as recited in claim 33 wherein the digital good includes one or

more of: a software program, audio content, and video content (see Sirbu, col. 1,

lines 13-25).

5.   Claims 7 and 14 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Merkle (U.S. Patent No. 5,003,597) and Chow (U.S. Patent

No. 6,594,761) and further in view of Sirbu (U.S. Patent No. 5,809,144).

In respect to claim 7, Merkle and Chow disclose one or more computer

readable media as recited in claim 1. Merkle and Chow do not explicitly

discloses wherein the digital good includes video content. However, Sirbu

discloses encrypting video content of digital goods. It would have been obvious

to one of ordinary skill in the art at the time the invention was made to implement

the teaching of Merkle's encryption technique to encrypt video content for secure

data transmission over the insecure Internet.

In respect to claim 14, the claim limitation is a method claim that is

substantially similar to computer readable media claim 7. Therefore claim 14 is

rejected based on the similar rationale.

Conclusion

6.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

-Adams et al. Discloses a practical s box design.

-Candelore et al. Disclose a secure processor with external memory using

block chaining and block re-ordering.

-Yasukawa et al. Disclose method and apparatus for protecting widely

distributed digital information.

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Tongoc Tran whose telephone number is

(703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789.

The fax phone number for the organization where this application or proceeding

is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).

Examiner: Tongoc Tran
Art Unit: 2134

TT

2004-04-20

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137